JOURNAL OF NUMBER THEORY 4, 269–273 (1972)

Representations by k-th Powers in $GF(q)$†

G. T. DIDERRICH AND H. B. MANN

Department of Mathematics, University of Arizona, Tucson, Arizona 85721

Communicated August 3, 1970

A lower bound is computed for the number of elements of a finite field F represented by

$$a_1x_1^k + \cdots + a_lx_l^k,$$

where $a_i \neq 0$ are fixed elements of F and $(x_1, \ldots, x_l)$ varies over F^l.

1. INTRODUCTION

In this paper we estimate the number of elements represented by a form $a_1x_1^k + \cdots + a_lx_l^k$, $a_i \neq 0$ in a finite field $GF(q)$. In particular, we prove a generalization of a theorem of Chowla, Mann, and Strauss (cf. [1] and Theorem 2.1 of [2]). We shall use the terminology and notation of [2].

THEOREM 1. *Let $GF(q)$ be a finite field where $q = p^n$ and p is a prime. Let k be a positive integer and set $k_1 = \text{g.c.d.}\ (k, q-1)$ and $s = (q-1)/k_1$. Let $a_1, \ldots, a_l$ be l nonzero elements of $GF(q)$ and let Y be the set of all elements in $GF(q)$ represented by the form $a_1x_1^k + \cdots + a_lx_l^k$. If $k_1 \leqslant p$ and $k_1 < (q-1)/2$, then either $Y = GF(q)$ or $|Y| \geqslant (2l-1)s + 1$.*

COROLLARY *If $l \geqslant (k_1+1)/2$, then every element of $GF(q)$ can be represented by the form $a_1x_1^k + \cdots + a_lx_l^k$.*

Theorem 1 and the corollary follow from J. H. B. Kemperman's generalization of Vosper's theorem (c. f. Theorem 5.1 of [3] and Theorem 1.3 of [2]) and from simple extensions to Lemmas 2.1.1, 2.1.2, and 2.1.3 of [2].

2. PROOF OF THEOREM 1

If A, B are nonempty subsets of an Abelian group G (written additively), we denote by $A + B$ the set of sums $a + b$, $a \in A$ and $b \in B$. We denote

† Sponsored by the United States Army under Contract No. DA-31-124-ARO-D-462.

641/4/3-4

by $H(A)$ the subgroup of G consisting of all elements $g \in G$ for which $g + A = A$. The set A is called periodic with period $H(A)$, if $H(A) \neq \{0\}$, otherwise it is called aperiodic.

DEFINITION. A subset B of G is called quasi-periodic with a quasi-period F, if there exists a subgroup F of G of size $|F| \geqslant 2$ and two subsets B' and B_1 of B satisfying the conditions:

(i) $B = B' \cup B_1$, and $B' \cap B_1 = \varnothing$,
(ii) $B' \neq \varnothing$ and $B' + F = B'$,
(ii) $B_1 \leqslant b_0 + F$ where $b_0 \in B_1$.

B' is called the periodic part of B, and B_1 is called the residual F-coset of B (cf. Sections 1 and 2. of [3]).

LEMMA 2.1. *Let* $X = \{x_1, ..., x_s\}$ *be an aperiodic set of elements of* $GF(p^n)$, $p > 3$ *with* $s > 1$, $s \not\equiv -1 \pmod p$, *and* $\sum x_i = \sum x_i^2 = 0$ *(sum over* X*). Then*

(a) *X is not in arithmetic progression.*
(b) If X is quasi-periodic with residual set X_1 of size $|X_1| > 1$, then X_1 is not in arithmetic progression.

Proof. For (a), assume X is in arithmetic progression with difference $d \neq 0$, $X = \{a_0, a_0 + d, ..., a_0 + (s-1(d\}$. The condition $\sum x_i = 0$ implies $\sum a_0 + (i-1)d \equiv 0 \pmod p$, hence $a_0 \equiv d(s-1)/2 \pmod p$. The condition $\sum x_i^2 = 0$ gives

$$\sum (a_0 + (i-1)d)^2 \equiv d^2\left(\frac{(2s-1)\,s(s-1)}{2\cdot 3} - \frac{s(s-1)^2}{2} + \frac{s(s-1)}{2^2}\right) \equiv 0 \pmod p. \tag{1}$$

Since X is aperiodic we have $s \not\equiv 0 \pmod p$.
Simplifying (1) gives $s + 1 \equiv 0 \pmod p$, a contradiction. For (b) assume X is quasi-periodic with residual subset X_1. Observe that $\sum x_i = \sum x_i^2 = 0$ over the periodic part of X, therefore $\sum x_i = \sum x_i^2 = 0$ over X_1. Applying (a) gives (b).

LEMMA 2.2. *Let k be a positive integer satisfying* g.c.d.$(2k, q-1) < q-1$, *then the nonzero k-*th *powers $x_1, ..., x_s$ in $GF(q)$ satisfy $\sum x_i = \sum x_i^2 = 0$. Further, let $a_1, ..., a_l$ be l nonzero elements of $Gf(q)$ and let*

$$Y = \{y \mid y = a_1 x_1^k + \cdots + a_l x_l^k\}, \qquad \textit{then} \qquad \sum_{y \in Y} y = \sum_{y \in Y} y^2 = 0.$$

Proof. Let w be a primitive root of $GF(q)$. The group generated by w^k consists of the nonzero k-th powers. The order of w^{2k} is

$$\frac{q-1}{\text{g.c.d.}(2k, q-1)}.$$

The hypothesis of this lemma implies $w^{2k} \neq 1$, hence $w^k \neq 1$. Now $(\sum x_i)\, w^k = \sum x_i$, therefore $\sum x_i = 0$. Similiarly we show $\sum x_i^2 = 0$. For the second part, note $Yw^k = Y$, then apply the same argument.

LEMMA 2.3. *Let $a_1, \ldots, a_l$ be l nonzero elements of $GF(q)$ and let $Y = \{y \mid y = a_1x_1^k + \cdots + a_lx_l^k\}$. Set $k_1 = \text{g.c.d.}(k, q-1)$, then $\mid Y \mid \equiv 1 \pmod{s}$ where, $s = (q-1)/k_1$. Furthermore, if $k_1 > 1$ and Y is periodic, then $\mid H(Y) \mid > q/k_1$.*

Proof. Let X be the multiplicative group of nonzero k-th powers in $GF(q)$. Then the group X operates on Y by multiplication. Since the isotropy group is $\{1\}$ for each nonzero orbit yX, it follows that all the orbits are of the same size $\mid X \mid = s$ (cf. pp. 19–23 of [4]). This implies $\mid Y \mid \equiv 1 \pmod{s}$.

For the second part, let $H = H(Y)$ and let h be a nonzero element of H. Now $YX = Y$ and $h + Y = Y$, therefore

$$(Y + h)X = YX + hX = Y + hX = Y,$$

hence $hX \subseteq H$. Thus $\mid H \mid \geqslant 1 + s$, but

$$s = \frac{q-1}{k_1} \quad \text{and} \quad 1 + \frac{q-1}{k_1} > \frac{q}{k_1} \quad \text{if} \quad k_1 > 1.$$

We can prove Theorem 1 by induction on l. For $l = 1$ the statement is obviously true. Assume $l \geqslant 2$, let $A = \{y \mid y = a_1x_1^k + \cdots + a_{l-1}x_{l-1}^k\}$ and let $B = \{y \mid y = a_lx_l^k\}$. We have

$$\begin{aligned} &\mid A \mid \geqslant \min(q, (2l-3)s + 1), \\ &\mid B \mid = s + 1. \end{aligned} \tag{2}$$

If $C = A + B$ is periodic, Lemma 2.3 implies $\mid H(C) \mid > q/k_1$; however, $k_1 \leqslant p$; therefore, $C = GF(q)$. Thus we may assume C is aperiodic; then by Kneser's Theorem (cf. Theorem 1.5 of [2] and Theorem 3.1 of [3]), we have

$$\mid C \mid \geqslant \mid A \mid + \mid B \mid - 1. \tag{3}$$

If $|C| = |A| + |B| - 1$, then by Kemperman's Theorem 5.1 [3] we conclude:

(a) Either (A, B) is an elementary pair, or

(b) (A_1, B_1) is an elementary pair where both A, B are quasi-periodic with the same quasi-period F and A_1, B_1 denote the residual F-cosets of A, B, respectively. We shall prove that neither (A, B) nor (A_1, B_1) is an elementary pair of type I, II, III, or IV of [3, Section 5].

For the type I possibility (using Lemma 2.3), we have an equation of the form

$$1 + Lp^m = 1 + T\left(\frac{p^n - 1}{k_1}\right), \quad 1 \leqslant m < n, \quad L \geqslant 1, \quad \text{and} \quad T \geqslant 1. \tag{4}$$

Therefore, $p^m \mid T$, since $p^m \nmid (p^n - 1)/k_1$. Hence $T \geqslant p$ and since $k_1 \leqslant p$, this gives $1 + T(p^n - 1)/k_1) \geqslant p^n$, a contradiction because $A + B$ is aperiodic.

For the type II possibility, Lemmas 2.1 and 2.2 imply if either B or B_1 is in arithmetic progression their size must equal $p - 1$. However, since neither $|A| = 1$ nor $|A_1| = 1$, it follows that $A + B$ must be periodic, a contradiction.

The type III possibility is ruled out since we are assuming $A + B$ is aperiodic.

The type IV possibility implies that $C = A + B$ is a union of F-cosets plus one residual F-coset C_1 which can be obtained from $c_0 + F$ by deleting c_0. Therefore $c_0 \notin C$; however, by Lemma 2.2 we have $\sum c_i = 0$ (sum over c) and $c_0 + \sum c_i = 0$ because we are summing over full F-cosets. Therefore $c_0 = 0$, a contradiction.

Therefore in (3) we must have

$$|C| \geqslant |A| + |B|$$

and

$$|C| \geqslant (2l - 2)s + 2.$$

Finally, Lemma 2.3 implies

$$|C| \geqslant (2l - 1)s + 1,$$

completing the proof.

The corollary follows since $l \geqslant (k_1 + 1)/2$ implies $(2l - 1)s + 1 \geqslant q$.

Remark. If $k_1 > p$, then the k-th powers can lie in a proper subfield of $GF(q)$; e.g., take $k = (q - 1)/(p - 1)$ then all the k-th powers reside

in the prime field of $GF(q)$; thus to obtain a theorem analogous to Theorem 1, one must put restrictions on the coefficients $a_1, \ldots, a_l$.

Also note that in Theorem 1 the condition $k_1 < (q-1)/2$ is necessary to obtain the bound $(2l-1)s+1$ because $2k_1 = q-1$ implies the k-th powers are in arithmetic progression with difference 1, i.e., -1, 0, 1, and application of Kneser's Theorem gives only the bound $ls+1$.

References

1. S. Chowla, H. B. Mann and E. G. Straus, Some applications of the Cauchy–Davenport theorem, *Norske Vid. Selsk. Forh. Trondheim* **35** (1959), 74–80.
2. H. B. Mann, Addition theorems, *in* "The Addition Theorems of Group Theory and Number Theory," Interscience, New York, 1965.
3. J. H. B. Kemperman, On small sumsets in an Abelian group, *Acta Math.* **103** (1960), 66–88.
4. S. Lang, "Algebra," Addison–Wesley, Reading, MA, 1965.